Contents

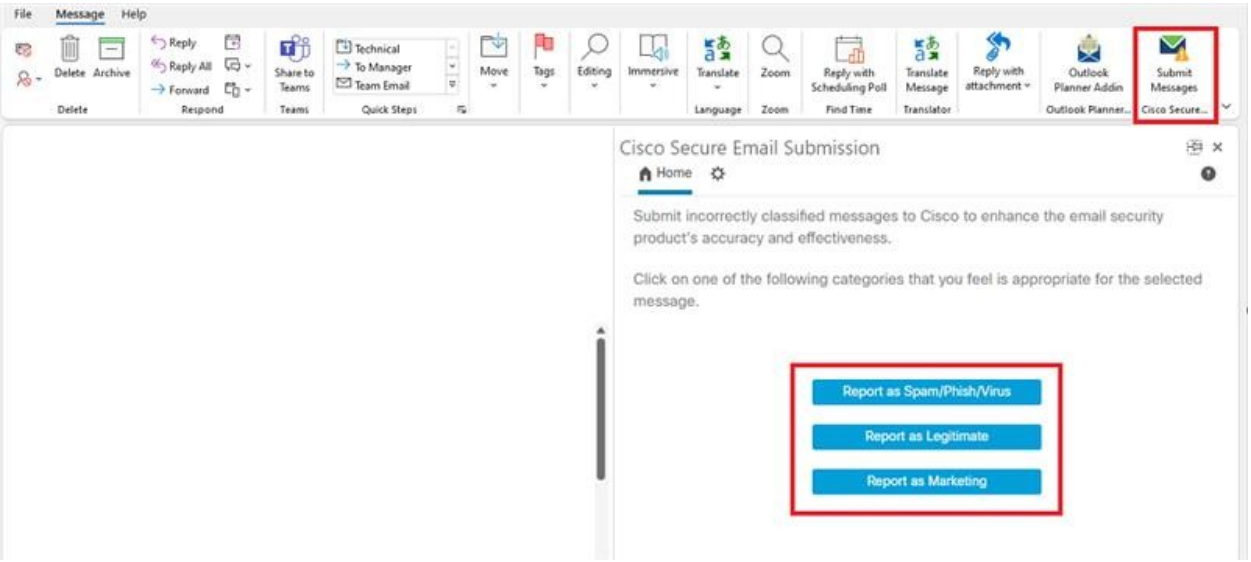
1. **Process needs to be followed for getting email file from associate and Messaging Team**
2. **Guidelines to be followed for Phishing Investigation analysis**
3. **Phishing Reported Email - Should be followed up till 2nd reminder only - For GWS emails.**

1. Process needs to be followed for getting email file from associate and Messaging Team

a. When associate informing that he/she have received suspicious email

Steps

1) Inform associate to report email by clicking “Submit Message” and choose either of the highlighted Option if associate is using Outlook.



Incase associate is using Gmail, inform associate to follow below steps to download email to his computer and share that email as attachment for further investigation.

- On your computer, go to Gmail.
- Open the email.
- Click More More.
- Click Download message.

Send emails as attachments.

- Click Compose.
- At the bottom, click Attach files and attach respective file.

- Select the file and click Open.
- Click Send

Important: To open the EML file that downloads, you need a desktop mail client.

b. When messaging team informing that associate have received suspicious email

Steps

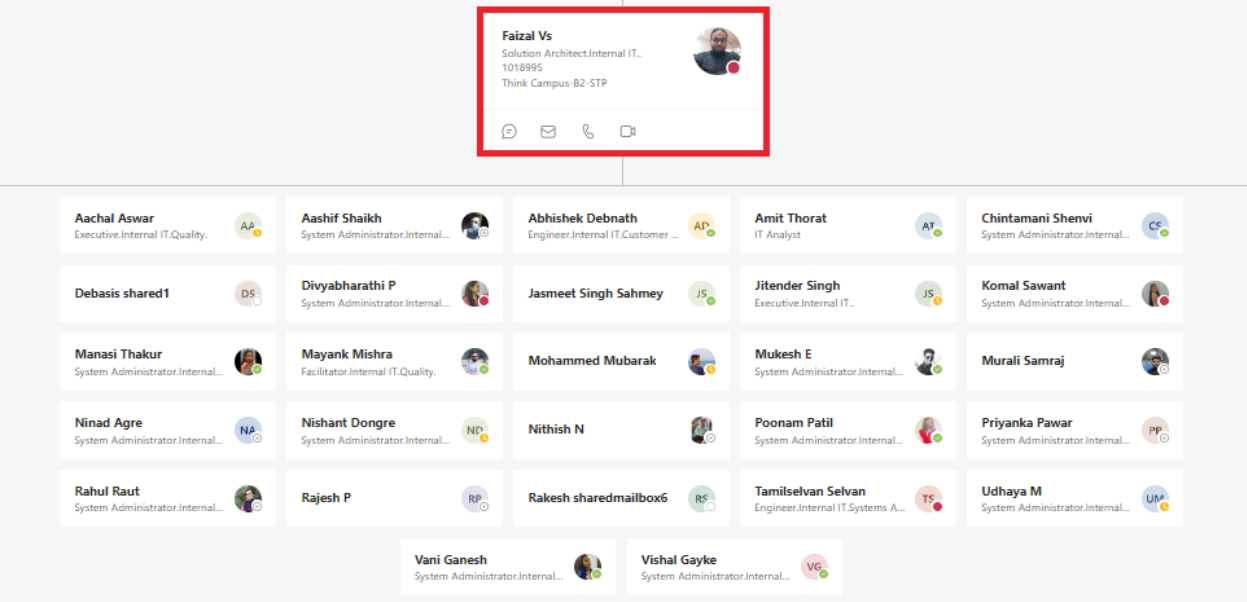
1) Inform associate to report email following either of the above steps.

Or

1) Inform messaging team to share .eml file of that email.

2) Keep follow-ups with associate/messaging team every 30 mins till we receive eml file, adding his supervisor in second reminder.

Simultaneously, to get details quickly connect respective associate or messaging team person available over Teams Chat who can share the file.



2. Guidelines to be followed for Phishing Investigation

Subject-Reported Email Investigation- User/GWS/ Email Gateway (FE)/SOAR-Incident No.-

1) Management Summery

- **Short Summery** of reported email content.
- **Verdict** of Investigated Email
- **Recommendations**-To block sender id, domain or any other.
- **Email Snapshot** displaying content.
- **Sender Signature** Details
- **Attachment of Original Email, IronPort logs, Investigation Report.**

2) Header Analysis

- **Sender IP Details** along with IP reputation information from TCS TIP, Virus Total, Abusedb, IPVoid, BrightCloud and RF.
- **Sender Domain Details** along with domain reputation information from TCS TIP, Virus Total, URLVoid, BrightCloud and RF.
- **Sender Domain Hosted IP Details** along with IP reputation information from TCS TIP, Virus Total, Abusedb, IPVoid, BrightCloud and RF.
- **X-Sender Domain Details** along with domain reputation information from TCS TIP, Virus Total, URLVoid, BrightCloud and RF.
- **X-Sender Domain Hosted IP Details** along with IP reputation information from TCS TIP, Virus Total, Abusedb, IPVoid, BrightCloud and RF.
- **Reply-to Domain Details** along with domain reputation information from TCS TIP, Virus Total, URLVoid, BrightCloud and RF.
- **Reply-to Domain Hosted IP Details** along with IP reputation information from TCS TIP, Virus Total, Abusedb, IPVoid, BrightCloud and RF.
- SPF, DKIM & DMARC Status (PASS/FAIL)

3) Content Analysis

- **URL Analysis**
    1. Screenshots of each URL browsing in MS Edge Isolation, Browserling, UrlScan.IO and sandbox verdict from all tools TCS TIP, Virus Total, URLVoid, BrightCloud and RF.
- **Attachment Analysis**

    1. Attachment Sandbox reports from both tools must be attached without fail. (FireEye and Wildfire)

4) Email Log Analysis

- **Email Delivery**-No. of Emails observed in IronPort console along with status-Delivered, Queued, Quarantined, Dropped etc. from sender id, subject name and with attachment name if any in last 30 days.
- **Delivery to Executives**- Email received by associates has any Executive associate as per our executive list in MS Team then call and inform SOC Manager.

5) Indicator of Compromise (IOCs)

- Hash
- IP Address
- URL
- Domain
- Email

6) Blocked IOCs

- Hash
- IP Address
- URL
- Domain
- Email

7) Presence of IOCs

- **Hash**
- **URL**
- **IP Address**
- **Domain**

8) Communication

- Communication to URLs/domains whether associates accessed it or not in our environment and those are allowed and blocked. If allowed, any suspicious activity observed in that user host.

9) IMT Details-Mandatory for all Phishing, Malicious emails.

10) **Miscellaneous Observation**

- Mention any other observation if any.

---

3. Phishing Reported Email - Should be followed up till 2nd reminder only - For GWS emails.

It has been observed that the team keeps following up on phishing reported email to get eml file while there is no response from respective associate who reported email. Henceforth, the team should not follow up with associate beyond two reminders. SCOC team must follow the steps below.

1) Create Manual Incident for Reported Email in SOAR

2) Email should be sent to associate for eml file with incident no. in subject and his/her supervisor, messaging team, associate location IS Group mail ID in CC.

Example-

Subject: Case number - Please share eml file for investigation (Emp id)

3) Reminder Email-If there is no response from associate then keep his/her supervisor in To.

Example-

Subject: First reminder – Case number - Please share eml file for investigation (Emp id)

4) If there is still no update then send final email as follows

Example-

Subject: Final reminder – Case number - Please share eml file for investigation (Emp id)

Email Content-

“Hi (Associate name),

We tried reaching you multiple times to get email copy of phishing email reported by you for investigation purpose but there is no response from your end, accordingly we are closing this case.

In case you get chance to download and share eml file then we will do further investigation of this email.

(Share procedure to download email copy for Gmail so there is no confusion with associate)”